Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Saturday, December 27, 2008

Bit gold markets

The basic idea of bit gold is for "bit gold miners" to set their computers to solving computationally intensive mathematical puzzles, then to publish the solutions to these puzzles in secure public registries, giving them unique title to these provably scarce and securely timestamped bits. These titles to timestamped bits will be more secure and provably scarce than precious metals, collectibles, and any other objects that have ever been used as money. In a description of bit gold, which was mostly an overview of the technology, I wrote about how, because the algorithms and architectures for solving computationally intensive mathematical puzzles to create bit gold will often be dramatically improved, the bits (the puzzle solutions) from one period (anywhere from seconds to weeks, let's say a week) to the next are not fungible. But fungible units can be created from non-fungible ones:

> bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today [pooling commodities with a wide variety of qualities into a handful of standard grades] to make commodity markets possible.

Bit strings (puzzle problem/solution pairs) are securely timestamped by their time of publication. More recent solutions that have been produced in greater quantities will be discounted by markets. To create fungible units dealers will bundle strings of different value into pools of a standard value (i.e. collect strings into a pool so that the sum of the market values of the strings in the pool add up to the standard value).

It's a bit indirect, but computers can easily handle these logistics. Leaving aside the gold metaphor for a minute, one can think of these bit strings as digital rare postage stamps. Each stamp might trade for a different price, but one can sort stamps into pools so that the prices of stamps in each pool add up to the same total price. Then divide each pool into tranches to create your standard currency denominations.

The rare stamp metaphor is, however, in other ways very misleading. Unlike stamps, but like gold, there are no ongoing changes in subjective valuations between bit strings to worry about, but instead the demand for bit gold is purely for its monetary functions, and thus purely based on how scarce the supply of puzzles solved during a given time period was and is. As a result, pooling and tranching will work far better for bit gold than it does for actual rare postage stamps.

This deserves more elaboration. It seems to be a common objection to bit gold that the mere difference in the price of a bit from one time period to the next produced by technology improvements introduce intractible subjective valuations, making the matter of

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

comparing one week to the next subject to too much uncertainty and transaction costs, as occurs with many collectibles. Just as pooling and tranching rare postage stamps would be a somewhat risky affair as subjective valuations of the underlying stamps change, so too this is supposed for bit gold.

The problem that would occur if we tried to turn most collectibles into a standard currency by pooling and tranching is that, besides a subjective aesthetic component in the demand curve that doesn't come into play with computer bits, their scarcity is uncertain. Art can turn out to be forged, rare stamps thought to be lost or to have never existed might be found, and so on. The supply curve, in other words, can be highly uncertain and in danger of elasticity. Since the supply and demand curves of different pools can change differently over time, the relative values of pools would diverge from their initial values, so that trying to use tranches as standard denominations of a currency would create arbitrage opportunities.

By sharp contrast bit gold will be entirely public: no one gains secure title to any puzzle solutions until they are published. Thus, the exact amount and kind of puzzle solutions during a given period are well known, and perfectly define the supply curve relative to future weeks for all time thereafter.

There will be, in other words, a perfectly objective, measurable, and inelastic supply curve, completely derivable from the relative scarcity of bits (puzzle solutions) on the week (or the day, or the hour, or the minute, if necessary) of their publication. Arbitrage to set the different prices of different weeks (or minutes) can be computerized on this basis. The demand curve, the demand for puzzle solutions for the monetary functions they can perform as a store of value and medium of exchange, will be based on recognition of the superiority of bit gold as a form of money that is more secure and has a far less elastic supply curve than traditional commodities such as precious metals. Since there are no aesthetic differences, the demand curve will be the same function of scarcity for all weeks (or minutes), so it won't affect the simple scheme of automated arbitrage between epochs with different supply curves. The supply and demand curves of different pools will change in the same way over time, and the relative values of pools will not diverge from their initial relative values. Using tranches as standard denominations for a currency does not create arbitrage opportunities.

For most of history collectibles were used for as stores of value and media of exchange; aesthetics played an important role. But before we can separate out the roles of scarcity and aesthetics, we must ask why humans evolved such aesthetic values. The aesthetic instincts, for example the instinct to collect shiny things, evolved just because in the evolutionary environment they approximated an instinct to collect scarce things, and to distinguish hard-to-find from easy-to-find things, i.e. an instinct to recognize and collect objects that can best perform monetary functions, as I describe here, in the "Evolution..." section early in the paper, and the "Attributes of Collectibles" section late in the paper.

As a proximate matter, the contribution to the demand curve from demand for monetary functions (store of value or medium of exchange or both) and the contribution from aesthetic considerations are completely separable. One can demand a commodity for its aesthetic value, or for its value as money, or for both, or for neither. Thus a check for a million dollars might have a design that is utterly philistine, yet the check is still worth a million dollars.

The value of gold today is almost entirely based on its monetary value rather than mere aesthetic value. There are plenty of metals that are as shiny and smooth as gold, but people don't demand them as a store of value or medium of exchange because they are common. There are plenty of rocks that look as good as diamonds, but "diamonds are a girl's best friend" because they are hard to obtain and thus hold their value. Value comes to attach to the unique aesthetic features of gold or diamonds because these features signal scarcity. The value of precious metals or gems as stores of value, media of exchange, or even as cultural icons does not come from these aesthetic features, it is only signalled by them. It is their secure scarcity, not their aesthetic features, that allows them to be more securely used as a store of value and thus gives them a monetary value, and often a corresponding emotional and cultural value, far above the often trivial value they would have if they had the same aesthetics but were common.

There will be a problem defining futures contracts for yet-to-be produced bit gold: how much it might cost to solve a given puzzle a

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ▼ 2008 (55)
  - ▼ December (2)
    - Bit gold markets
    - Bit gold
  - ► October (2)
  - ► September (4)
  - ► August (9)
  - ► July (4)
  - ► June (6)
  - ► May (6)
  - ► April (4)
  - ► March (10)
  - ► February (5)
  - ► January (3)
- ► 2007 (47)
- ► 2006 (130)
- ► 2005 (44)

year later, or even a month, will be a very uncertain matter. But the pools that define currencies will be based on spot prices for already produced bit gold, not on futures.

[These comments edit and add to comments of mine under previous blog post(s)]

Posted by Nick Szabo at 4:17 PM

17 comments:

Anonymous said...

Nick,

Diamonds are, in fact, plentiful. http://www.theatlantic.com/doc/198202/diamond

6:46 PM

Byrne said...

Stipulating that a bit-gold standard would be voluntarily accepted rather than imposed, I suspect that it might be a competitive disadvantage. The problem is that there is an almost perfect linear relationship between trying to solve the puzzles (in the form of participating in projects analogous to SETI@home), so one could expect all the spare computer cycles in that society to be used for bit gold (and for extra computers to be thrown at the problem if it's easy enough at first).

At that point, bit gold is no longer backed by the scarcity of solved puzzles -- it's backed by the scarcity of computer hardware, power, and programmers who specialize in high-performance computing. In other words, it devolves into a very inefficient and wasteful basket-commodity standard.

7:40 PM

nick said...

Even if diamond scarcity had more to do with cartel behavior than with geology (it doesn't, but let's go with that), as long as people believe in the scarcity, they are still valuing the diamond almost entirely for its scarcity, not its sparkle. One can get nice sparkle from any number of cheap goo-gaws, but it won't be the sparkle of scarcity that signals true love.

As for why diamonds went retail, with the first and greatest success in the U.S., there's far more to it than De Beers ad campaigns. The most successful marketing campaigns identify and trigger already latent demand, they don't create demand from scratch. During the period diamonds took off in the U.S. there were changes in family law that made engagement and marriage less expensive commitments for men. Women demanded a credible substitute, collateral with monetary properties that didn't look too much like money, and got it.

7:45 PM

Michael Froomkin said...

Each stamp might trade for a different price, but one can sort stamps into pools so that the prices of stamps in each pool add up to

the same total price. Then divide each pool into tranches to create your standard currency denominations.

Hmmm... Sounds a bit like what they did in the mortgage market.

How certain are we that the person putting together the pool will not collude with the providers of the elements to include bits-gold pieces that are fakes?

Will the people taking the pools as funds or collateral have to check the validity of every element? What's the complexity and computational cost of that? If it's not low, is this both liquid and reliable?

8:13 PM

nick said...

Byrne: *bit gold is no longer backed by the scarcity of solved puzzles -- it's backed by the scarcity of computer hardware, power, and programmers who specialize in high-performance computing. In other words, it devolves into a very inefficient and wasteful basket-commodity standard.*

Per bit or per CPU cycle or per puzzle solved the costs of bit gold can come down quickly as technology improves or as more people start replacing SETI@home with BitGold@home -- that's why the bits generated one week are not, in contrast to atoms of gold, fungible with the bits generated next week -- the solution of which problem I describe in the post above: arbitrage, pooling, and tranching. The standard unit in bit gold is a tranch, for example a tranch of the pool of bits generated (puzzles solved) within a given week.

Bit gold is always backed by the scarcity of solved puzzles, but the puzzle solutions in a prior week are not of equal supply, and thus not of equal value, to the solutions of the next week. If all of a sudden ten times as many puzzles are being solved in week 52 as in week 51, they will be priced at about 10% of the value of the puzzles in week 51, and it will take 10 times as many puzzles to create the standard pool. Supply of *pools* is based on weeks: week 2 doubles the supply of pools over week 1, but week 100 can only increase the overall supply of pools by 1%, regardless of how many puzzles are solved.

All this is more wasteful than gold mining. CPU cycles spent generating bit gold get amortized over a large number of transactions using the commodity-based currency, just as occurs with the costs of gold mining. To be useful both gold and bit gold have to end up saving users more in transaction costs than is expended in the gold mining or the CPU running. They both save transaction costs by serving as stores of value and media of exchange, or as backing for fractional reserve currencies that do same, but bit gold will perform these monetary functions with greater security, lower storage costs, etc. than gold.

I suspect this is all obscure enough that (a) it may require most people to sit down and work it out for themselves carefully before it can be well understood, and (b) it would greatly benefit from a demonstration, an experimental market (with e.g. a trusted third party substituted for the complex security that would be needed for a real system). Anybody want to help me code one up?

8:53 PM

nick said...

How certain are we that the person putting together the pool will not collude with the providers of the elements to include bits-gold pieces that are fakes?

It's based on strong security, minimizing trust, in sharp contrast to mortgages where one must trust all the parties involved, depsite the often bad incentives (moral hazard) involved. The title registry, which holds the timestamp hash chains, solutions bits, etc. is public -- supply cannot be hidden. An overview of the security protocols involved is here, with links to further explanations.

8:58 PM

nick said...

I miswrote: *All this is more wasteful than gold mining.*

Ha ha! That was supposed to read "no more wasteful than gold mining."

To put my answer to Michael Froomkin another way, bit gold is based on an unforgeable auditing log, a chain of puzzles and solutions each of which is timestamped. The entire value chain from puzzle to solution, and all transfers of title, are available for all bit gold and can be audited by anybody at any time.

1:13 PM

George Weinberg said...

Ha ha! That was supposed to read "no more wasteful than gold mining."

That's hard to say. One philosophical objection to the idea of gold-based money is that the effort of mining and refining gold seems wasted. Presumably people will spend effort mining gold iff it pays better than using their time in other ways. But whether or not a given gold deposit can be profitably mined obviously depends on the quality of the deposit, and I think the initial finding of gold deposits is largely serendipitous. This would not be the case for bit gold. It would be as if mining gold anywhere is more or less equally profitable. It's not clear to me whether this would lead to more gold mining or less, but I could imagine it leading to vastly more.

The entire value chain from puzzle to solution, and all transfers of title, are available for all bit gold and can be audited by anybody at any time.

Is it possible to do this and somehow maintain privacy?

10:30 AM

Byrne said...

Hm. It looks like in your current explanation, the puzzle-solving cancels out: bit gold units = puzzles done in time period / ratio of these puzzles to puzzles done in a typical period. Why do the puzzling at all, rather than issuing a fixed amount of currency inflated at a predictable rate, with unique identifiers for each unit of currency?

It seems much more wasteful than gold mining for the reason I mentioned before: as long as the marginal benefit of extra bits is lower than the marginal cost of running computers, people will keep their computers running when they'd otherwise shut them down, to easily arbitrage this difference. This is far more wasteful than mining gold, especially because one would expect available computing power to grow faster than known gold deposits.

Given the choice between a society that invests non-sensible amounts in the presence of a shiny metal, and one that invests non-sensible amounts in the presence of spare computer cycles, the former seems like the more reasonable choice.

Even so, I'd rather just use baskets of ETFs as currency. Very low marginal cost, 'inflation' is easy to correct by switching to different ETFs depending on share issuance policies and the like. 'Currency' as a savings vehicle rather than a way to denominate transactions strikes me as a poor idea.

10:40 AM

nick said...

george weinberg: *One philosophical objection to the idea of gold-based money is that the effort of mining and refining gold seems wasted.*

Demand is based on savings in transaction costs from bit gold, from it being a better hedge or media of exchange than alternatives such as gold. (Because it is more secure against political problems, can be used online without going through trusted third parties like e-gold, has a completely measurable stockpile, etc.) The resulting savings in transaction costs, amortized over the ulimited lifetime of the bit gold, generally has to exceed these costs to create this demand. As with gold mining, there is a wide range of costs, and the scarcity matches the cost, so it's not a question of if there is a market for bit gold, only a question of how big that market might eventually become (the answer to which is highly uncertain, and mainly depends on the possibilities of political disasters to which bit gold is the best hedge).

I think the initial finding of gold deposits is largely serendipitous. This would not be the case for bit gold.

This depends on the mathematical puzzle, but most of the ones proposed (such as hash algorithms) are probabilistic in nature, so depend on luck as well well as skill.

Economically, the much more important factor is that some "miners" will have more spare cycles, better compilers, better algorithms, or in a big market even better custom-designed circuits than others. So there is the usual opportunity for a few of the best "miners" to make a profit, while the vast majority of people will find some other way to make a living, just as with gold or silver mining.

2:14 PM

nick said...

Byrne: *Why do the puzzling at all, rather than issuing a fixed amount of currency inflated at a predictable rate, with unique identifiers for each unit of currency?*

This is an interesting idea, something like the idea that the Fed should follow a simple algorithm rather than trying to outguess markets. But the real question for beating bit gold is how do we do this without having to put full trust in third parties? If we can figure that out, we've come up with something better than bit gold. ("We" as usual on this blog being just whoever wants to explore the possibility, not "the government" :-)

Real trusted third parties, whether central banks or private note issuers, have always been tempted to overextend and overinflate, although occasionally the reverse happens. They are also vulnerable to government takeoever. Any algorithm, like the gold standard of old, is likely to be modified in a "crisis": a trusted third party cannot make a strong credible commitment to keep running the same algorithm.

Possibly the money issuing algorithm could be run by many parties in parallel manner, a technique known as Byzantine agreement. Indeed, this is the same technique used to run the bit gold title registry. All participats would agree to (1) generate a fixed number of unique (large random) numbers each week, (or a number inflated by some predictable algorithm), and (2) assign each by some fair algorithm to one of participants. Each timestamped random number becomes a rare collectible, like postage stamps. I can see where this would work! It will take quite a bit of thinking over, though, as we've eliminated one of things that bit gold users can approximately prove, i.e. the original cost of the gold.

Byzantine security is far from perfect. In layman terms it just means that when everybody sends everybody else the same message, far more people have to be corrupted in order to fake the message than if the message is sent through one or a few people. Thus any given party is trusted only to a very small degree, but there is still that small degree of trust. There is a much stronger temptation here than with bit gold to inflate the currency, since it can now be costlessly "printed" instead of "mined": it's much more likely that a sufficiently large number of people could be corrupted. Still, it's an intriguing idea worth developing even if for no other reason than it gives us another concrete plan to compare bit gold to.

as long as the marginal benefit of extra bits is lower than the marginal cost of running computers, people will keep their computers running when they'd otherwise shut them down, to easily arbitrage this difference.

I'm sorry, but this doesn't make any sense to me: do you mean to say "higher than" rather than "lower than"?

Some computers are more energy efficient than others, some have more spare cycles than others, some algorithms and custom circuits will solve puzzles far faster than others, and so on, so there will be great differences in profitability, and as in gold mining the market will evolve towards only a few of the best specialists in puzzle solving making a reasonable profit. Indeed, the technological differences between chips and algorithms are likely to be far *greater* than with gold mines, which is why we can't make the bits themselves fungible from week to week in the first place: the technology improves too fast.

2:46 PM

George Weinberg said...

Demand is based on savings in transaction costs from bit gold, from it being a better hedge or media of exchange than alternatives such as gold. (Because it is more secure against political problems, can be used online without going through trusted third parties like e-gold, has a completely measurable stockpile, etc.) The resulting savings in transaction costs, amortized over the ulimited lifetime of the bit gold, generally has to exceed these costs to create this demand.

I don't think that's right. With physical gold, mining more gold may bring benefit to the miner but it decreases the purchasing power of gold already mined. I don't see why increasing the quantity of refined gold in the world should change transaction costs one way or the other.

I think something similar should be true with bit gold. Once there's enough bit gold in the world that discrete coin size isn't much of an issue it seems to me that increasing the amount of bit gold in circulation won't do anything to lower transaction costs, it'll just decrease the purchasing power of existing coins..

4:53 PM

nick said...

george: *With physical gold, mining more gold may bring benefit to the miner but it decreases the purchasing power of gold already mined. I don't see why increasing the quantity of refined gold in the world should change transaction costs one way or the other.*

This is true, a but it illustrates another way in which timestamped bit gold is superior to non-timestamped gold. Cheaper mining of gold per atom decreases the purchasing power of gold atoms already mined by that amount, but because of secure timestamping and inter-week arbitrage (i.e. not treating all bits as fungible), a new week's worth of solved puzzles, regardless of how many or large the puzzles are that are solved, changes the value of preceeding weeks by a negligible amount in the long run. (BTW, for both gold and bit gold, spot prices already reflect expectations of how much will be produced in the future: but for gold this the number of atoms that will be produced, and for bit gold this an amortization of future weeks versus weeks of past stockpile already accumulated).

The same effect can already be observed in collectible coins: coins from eras in which coins were less seldom produced than today trade at increasing premiums over their value as gold. Even if we discovered a way to transmute lead into gold for free, these old coins would never lose their proof of scarcity -- they would only lose their gold value, but never their value as rare collectibles (which in the rarer epochs is far greater than the value of their gold atoms). That's as close as we can come to time-stamping gold.

1:39 PM

eddie said...

I don't think you need provable cost. You need provable scarcity. And if your scheme has a byzantine registry, you're there already -

you don't even need a method for generating and allocating random numbers. If there is a registry that establishes ownership of a number by a participant, then there must be a means of identifying participants - and that's all you need. Participants own their own identity.

A participant's ID becomes a coin, which they can trade as usual. Anyone who owns a coin can revoke it and issue new coins as change - the new coins are the old coin with bitstrings appended, such that the appended bitstrings completely partition the subspace. The value of any coin is then simply 1/(2^N) where N is the length of the coin (not counting the original issuer ID). For example, you could split the coin X into the coins X00, X010, X011, X10, X11, creating three +2-bit coins and two +3-bit coins. All this gets tracked in the registry.

This scheme has a (mostly) fixed amount of money that can be split into arbitrarily small denominations (and pooled and tranched into arbitrary denominations of any size). It's only mostly fixed, though - the amount of money is equal to the number of participants, and grows as the participant pool grows. Thus, the basic monetary unit is the lifetime of a person.

A similar scheme could be that each participant can issue new coins whenever they want; each coin would have a serial number, and serial number + issuer would be globally unique. Coins could still be split as before; the splitting digits would be separate from the serial number and issuer identifier. Again, the registry provides proof of scarcity. The value of coins would be measured in participant-seconds: the number of seconds between the coin's registration timestamp and the registration timestamp of the immediately prior registered coin from the same issuer. If I issued one coin a day each would be worth one person-day; if I issued two coins a day each would be worth half a person-day (on average, that is; each would be worth a specific, exact amount depending on exactly when they were issued). Now the monetary base grows both with the population and over time, so that on day 10,001 of the scheme there's .01% monetary growth from the day before. This is similar to your idea of pooling and tranching bitgold into standard-sized time-based chunks. Also, now the basic monetary unit is one day of a person's lifetime (or one second, or one year, etc.) instead of a person's entire lifetime.

With bitgold, the basic monetary unit is the cpu instruction cycle. To prevent ever-cheaper cpu cycles from causing inflation, your pooling idea then bundles cpu cycles into weeks (or days, or seconds), which become the new basic monetary unit. I think the person-second is a better fundamental unit, but if you prefer just plain seconds you can still get them without having to waste cpu cycles solving puzzles: use my person-second scheme, but stipulate that a coin's value is proportionate to the number of registered participants at the time of the coin's timestamp. In other words, my half-a-person-day coin would be worth 1/28th of a day if there were fourteen participants in the registry on the day the coin was registered. Now the monetary base grows strictly by time (adding equal amounts every time period), and the growth is distributed evenly among all participants.

8:35 PM

Barlycorn, John said...

I think a more appropriate name would be "bit wampum"

6:47 PM

Daniel A. Nagy said...

"*the demand for bit gold is purely for its monetary functions*"

But that leaves a huge bootstrap problem to be solved. Right now, bit gold has no monetary function, so there is no demand for it.

All the monetary instruments that we use are demanded either for some intrinsic value or because they backed by some desirable promise or because they are forced upon us (e.g. being the only thing in which we can pay our taxes).

Also, I still don't get how quantity and exchange rate are related. If there are twice as many puzzles solved next year than this year, it would make this years puzzle worth twice as much? What makes the relationship between quantity and exchange rate linear?

1:09 AM

Liberty said...

I buy and sell bitcoins, a real world bit gold implementation.

Getting Started
http://newlibertystandard.wetpaint.com/page/Getting+Started

Exchange Rate
http://newlibertystandard.wetpaint.com/page/Exchange+Rate

6:48 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.